Using the Embedded NGX EAP Authenticator

February 2008

Contents

Introduction **1**

How the Embedded NGX EAP Authenticator Works **3**

Workflow **4**

Configuring the Embedded NGX Appliance **7**

Configuring the Wireless Network 7

Configuring the Embedded NGX Appliance Ports 9

Configuring the SmartCenter Internal CA for Server Authentication 11

Exporting the Embedded NGX Appliance Certificate 13

Adding Network Access Users 14

Configuring Clients **16**

Configuring Clients for Server Authentication on Wireless Connections 16

Configuring Clients for Server Authentication on Wired Connections 19

Installing the Embedded NGX Appliance's CA Certificate on Clients 22

Connecting Wireless Clients to the Embedded NGX Appliance 26

Introduction

Wi-Fi Protected Access Enterprise (WPA-Enterprise) and 802.1x are Network Access Control (NAC) protocols that can be used to authenticate users connecting to the Check Point Embedded NGX appliance. Both WPA-Enterprise and 802.1x can be used to control access to the wireless network; however, WPA-Enterprise has the added capability of encrypting transmitted data, and 802.1x can be used to secure connections to the Embedded NGX appliance's LAN and DMZ ports as well.

Traditionally, WPA-Enterprise and 802.1x require installing an external Remote Authentication Dial-In User Service (RADIUS) server. When a user tries to authenticate using 802.1x or WPA-Enterprise, the Embedded NGX appliance sends the entered user credentials to the RADIUS server. The server then checks whether the RADIUS database contains a matching set of credentials. If so, then the user is logged on.

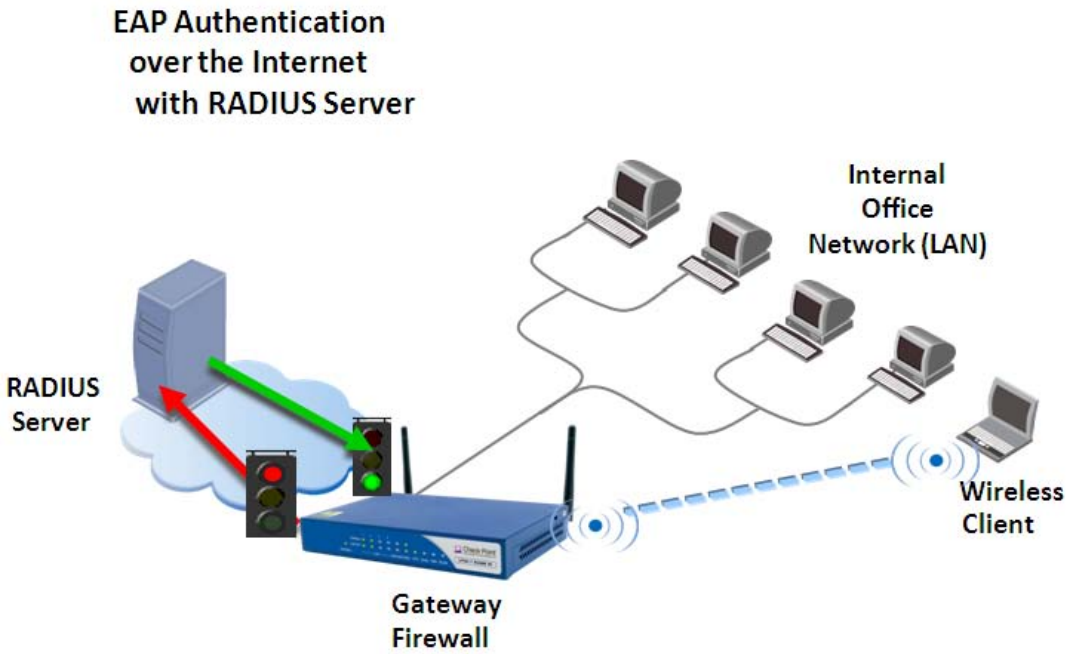


Figure 1: EAP Authentication with RADIUS Server

While purchasing and configuring a RADIUS server may pose little challenge for an enterprise, such a solution may be costly and complex, and may therefore be unsuitable for smaller businesses and home owners. In such cases, it is recommended to configure the Embedded NGX appliance's built-in Extended Authentication Protocol (EAP) authenticator, which allows using the local user database, enabling the use of WPA-Enterprise or 802.1x without an external RADIUS server.

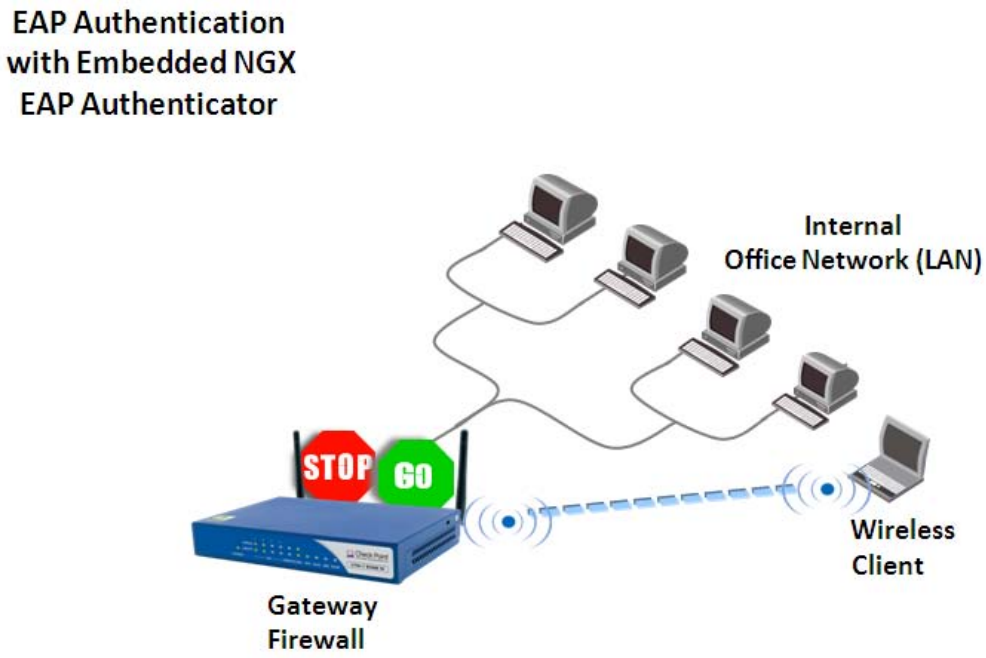


Figure 2: EAP Authentication with Embedded NGX EAP Authenticator

This document describes how to configure WPA-Enterprise and 802.1x security protocols with the Embedded NGX EAP authenticator.

Note: This document refers to Check Point Embedded NGX appliances version 8.0 or later. Embedded NGX gateways include Safe@Office, UTM-1 Edge, and ZoneAlarm Z100G gateways. The Embedded NGX screens that appear in this document relate to Safe@Office gateways.

How the Embedded NGX EAP Authenticator Works

The Embedded NGX EAP authenticator works as follows:

1. A client attempts to connect to the Embedded NGX appliance using 802.1x or WPA-Enterprise, either wirelessly or via a physical port.
2. The Embedded NGX appliance sends its certificate to the client.
3. The client verifies that the Embedded NGX appliance's certificate appears in its list of trusted CAs.
4. The client authenticates to the Embedded NGX appliance with its local user database username and password.

   The Embedded NGX appliance's built-in EAP authenticator searches the local user database for the authentication credentials and determines whether they are valid. The user must have “Network Access” permissions.
5. If valid credentials are found, access to the network is granted; otherwise, the authentication request is denied.
6. The authentication attempt is logged by the Embedded NGX appliance's Event Log.

Workflow

To use the Embedded NGX EAP authenticator

1. Configure the Embedded NGX appliance as follows:

   a. Do one of the following:

      - If configuring WPA or 802.1x for a wireless network, configure the desired wireless network's security protocol for use with the EAP authenticator.

        See ***Configuring the Wireless Network*** on page 7.

      - If configuring 802.1x for a LAN port or the DMZ port, configure the desired port for use with the EAP authenticator.

        See ***Configuring Embedded NGX Appliance Ports*** on page 9.

   b. Ensure that the Embedded NGX appliance has a certificate installed in the Embedded NGX Portal's VPN > Certificate page.

      The certificate can be any of the following:

      - A self-signed certificate generated by the Embedded NGX appliance, version 8.0 or later.

        If a self-signed certificate is installed on the appliance, but was generated by an earlier firmware version, you must generate a new certificate. For instructions on generating a self-signed certificate, refer to the User Guide.

      - A certificate received from the SofaWare Security Management Portal (SMP) version 7.0 or later

        In order to work with an SMP certificate, the SMP administrator must remotely install it on the Embedded NGX appliance. Alternatively, the SMP administrator can send you the certificate, which you must then import as described in the User Guide.

- A certificate received from Check Point SmartCenter

  In order to work with a SmartCenter certificate, the SmartCenter administrator must configure the SmartCenter internal CA for server authentication and then remotely install the certificate on the Embedded NGX appliance, as described in ***Configuring the SmartCenter Internal CA for Server Authentication*** on page 11. Alternatively, once the SmartCenter internal CA is configured properly, the SmartCenter administrator can send you the certificate, which you must then import as described in the User Guide.

c. Export the Embedded NGX appliance's certificate.

   See ***Exporting the Embedded NGX Appliance Certificate*** on page 13.

d. Send the certificate to all clients.

e. For each client that should be allowed to connect to the Embedded NGX appliance, add a user with Network Access permissions to the local user database.

   See ***Adding Network Access Users*** on page 14.

f. Provide each of the users with the authentication credentials you configured for them.

2. Configure each client as follows:

   a. Configure the client for server authentication, in one of the following ways:

      - If you configured WPA or 802.1x for a wireless network, see ***Configuring Clients for Server Authentication on Wireless Connections*** on page 16.
      - If you configured 802.1x for a port, see ***Configuring Clients for Server Authentication on Wired Connections*** on page 19.

b. Install the Embedded NGX appliance's CA certificate as a trusted root CA.

   See ***Installing the Embedded NGX Appliance's CA Certificate on Clients*** on page 22.

3. Do one of the following:

   - If you configured WPA or 802.1x for a wireless network, connect the wireless client to the wireless network.

     See ***Connecting Clients to the Embedded NGX Appliance*** on page 26.

   - If you configured 802.1x for a port, connect the client directly to the port, and enter the Network Access user's authentication credentials when prompted.

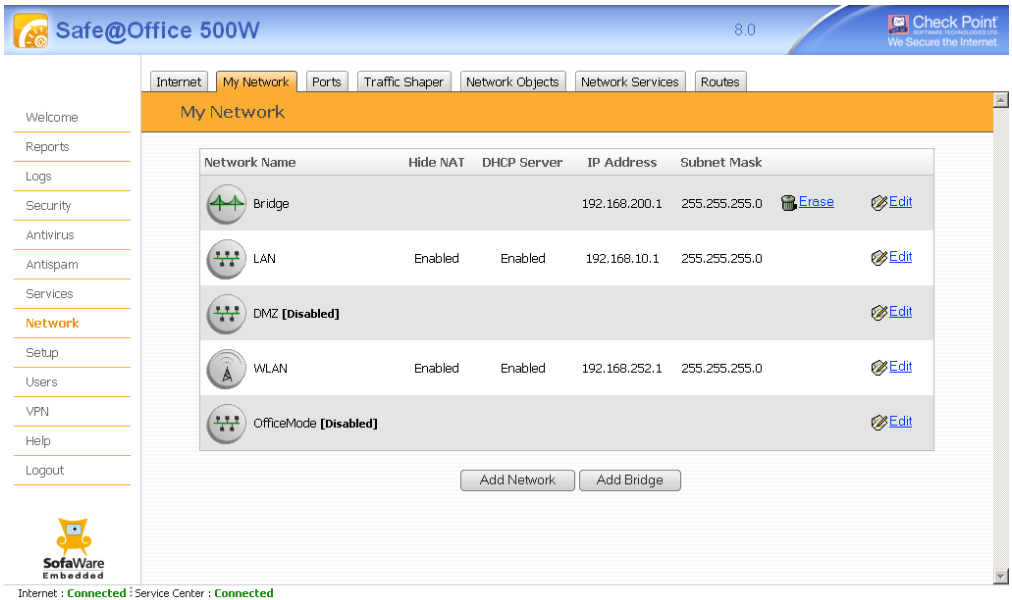
Configuring the Embedded NGX Appliance

Configuring the Wireless Network

To configure the wireless network

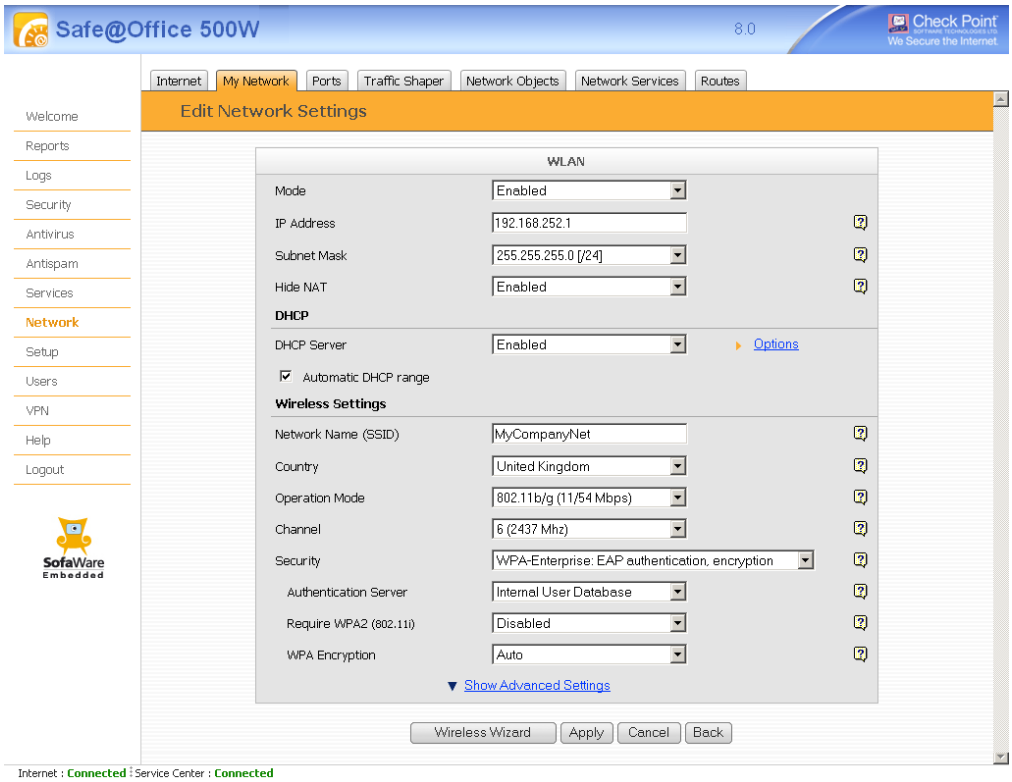
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.



2. In the desired wireless network's row, click Edit.

The Edit Network Settings page appears.



3. In the Mode drop-down list, select Enabled.

   The fields are enabled.

4. In the Security drop-down list, select the desired security protocol (WPA-Enterprise or 802.1x).

5. In the Authentication Server field, select Internal User Database.

6. Complete the rest of the fields as desired.

   For information, refer to the User Guide.

7. Click Apply.

Configuring the Embedded NGX Appliance Ports

To configure a port for a 802.1x security scheme

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to the desired port, click Edit.

The Port Setup page appears.

3. In the Assign to network drop-down list, select the network to which users should be assigned upon successful authentication.
4. In the Port Security drop-down list, select 802.1x.
5. In the Authentication Server field, select Internal User Database.
6. Complete the rest of the fields as desired.

   For information, refer to the User Guide.
7. Click Apply.

Configuring the SmartCenter Internal CA for Server Authentication

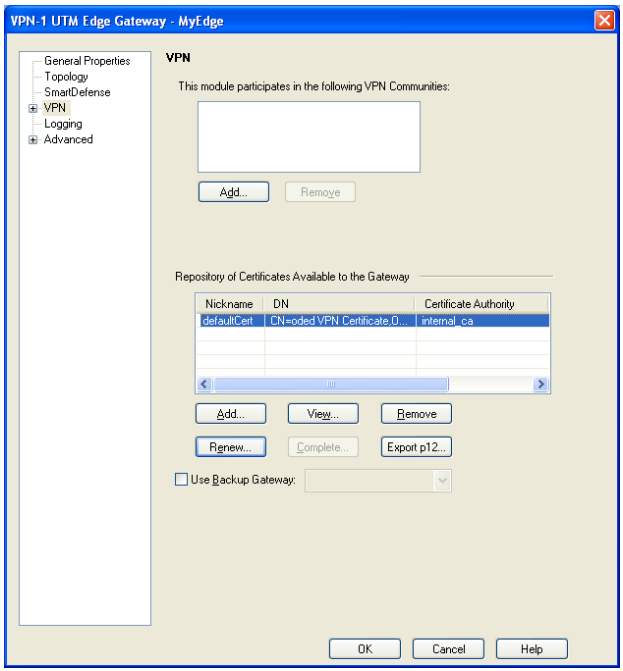
To configure the SmartCenter internal CA for server authentication

1. Perform a `cpstop` operation.
2. In the `$FWDIR/conf/InternalCA.C` file, add the `ike_cert_extended_key_usage` property with the value 1.
3. Perform a `cpstart` operation.
4. Renew the Embedded NGX appliance's certificate, by doing the following:
   a. In SmartDashboad or SmartLSM, open the gateway object representing the Embedded NGX appliance.

      The gateway object opens displaying the General Properties node.

   b. Click the VPN node.

The VPN node appears.



c. Click Renew.

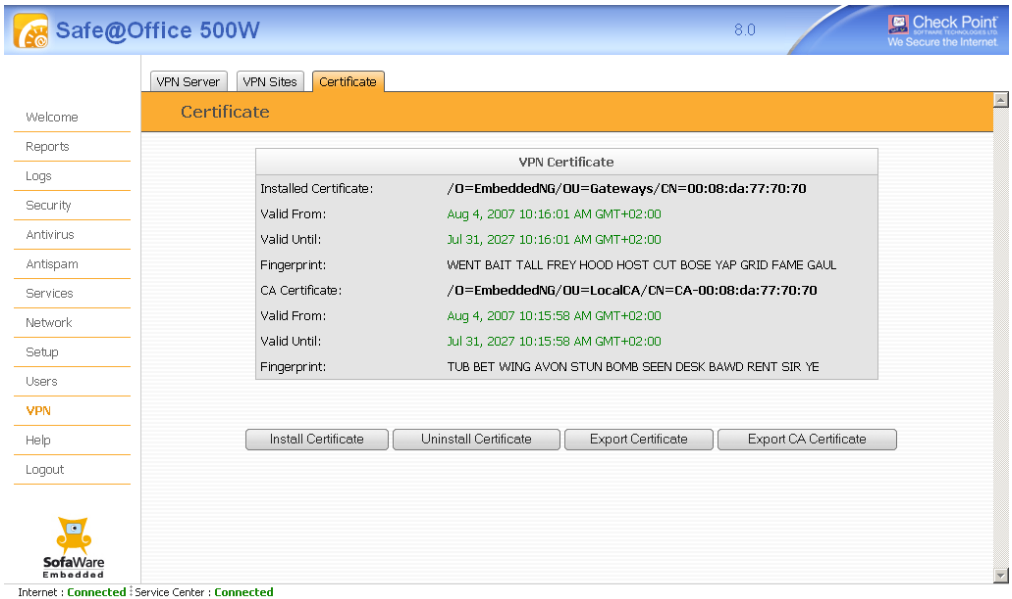
The new certificate is issued to the gateway.

Exporting the Embedded NGX Appliance Certificate

To export the Embedded NGX appliance's certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears.



2. Click Export CA Certificate.

   A standard File Download dialog box appears.

3. Click Save.

   The Save As dialog box appears.

4. Browse to a destination directory of your choice.

5. Type a name for the certificate file and click Save.

   The *.p12 file is created and saved to the specified directory.

Adding Network Access Users

To add a user with Network Access permissions

1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears.

2. Click New User.

   The Account Wizard opens displaying the Set User Details dialog box.

3. In the Username field, type the user name to use for authentication.
4. In the Password and Confirm password fields, type the password to use for authentication.
5. Copy down these authentication credentials.
6. Complete the rest of the fields as desired.

   For information, refer to the User Guide.

7. Click Next.

The Set User Permissions dialog box appears.

8. Select the Network Access check box.
9. Complete the rest of the fields as desired.

   For information, refer to the User Guide.
10. Click Finish.
11. The user is saved.

Configuring Clients

Configuring Clients for Server Authentication on Wireless Connections

To configure a client for server authentication

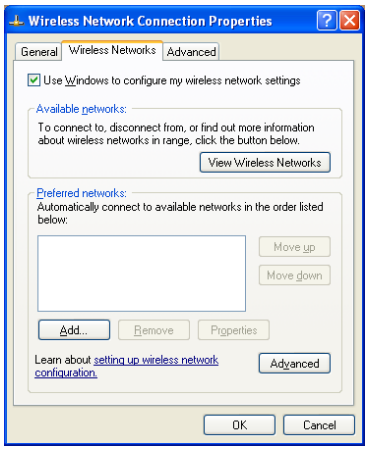
1. In the START menu, click Control Panel.
2. Click Network Connections.
3. Double-click on the wireless network connection.
4. Do one of the following:

   - If the Choose a Wireless Network screen appears, click Change Advanced Settings.
   - If you are already connected to a wireless network, click Properties.

   The Wireless Network Connection Properties dialog box appears displaying the General tab.

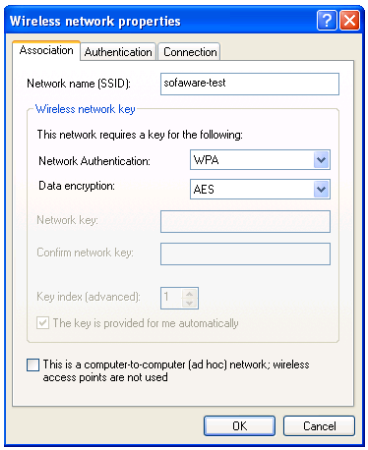
5. Click the Wireless Networks tab.

   The Wireless Networks tab appears.



6. Click Add and add your network.

   The Wireless network properties dialog box appears displaying the Association tab.

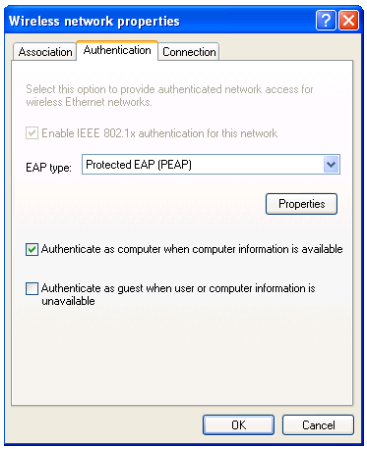


7. In the Network name (SSID) field, type the Embedded NGX appliance wireless network name.
8. In the Network Authentication drop-down list, select WPA.

   Note: You must select WPA, regardless of whether the Embedded NGX appliance is configured to use the WPA-Enterprise or 802.1x security protocol.

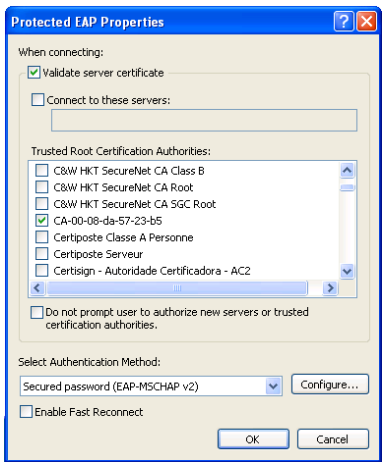
9. In the Data encryption drop-down list, select AES.
10. Click the Authentication tab.

The Authentication tab appears.



11. In the EAP type drop-down list, select Protected EAP (PEAP).
12. Select the Authenticate as computer when computer information is available check box.
13. Click Properties.

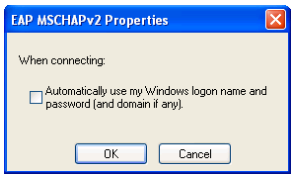
    The Protected EAP Properties dialog box appears.



14. Make sure that the Validate server certificate check box is selected.

15. In the Select Authentication Method drop-down list, select Secured password (EAP-MSCHAP v2).
16. If the user credentials for connecting to the Embedded NGX appliance differ from the user credentials for connecting to Windows, do the following:
    a. Click Configure.

       The EAP MSCHAPv2 Properties dialog box appears.



    b. Clear the check box.
    c. Click OK.
17. Click OK in all open windows.

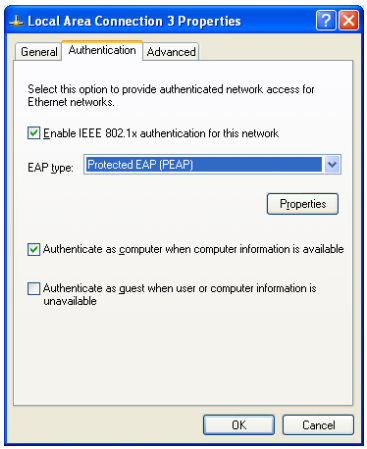
Configuring Clients for Server Authentication on Wired Connections

To configure a client for server authentication

1. In the START menu, click Control Panel.
2. Click Network Connections.
3. Right-click on Local Area Connection, and click Properties in the popup menu that appears.

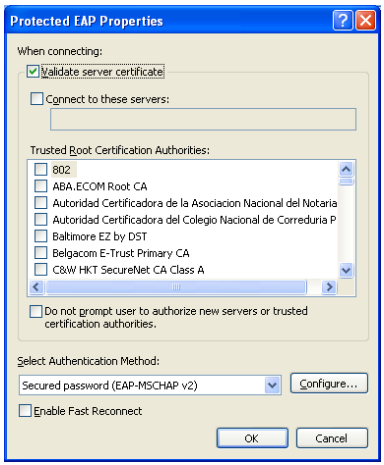
   The Local Area Connection Properties dialog box appears displaying the General tab.
4. Click the Authentication tab.

The Authentication tab appears.


Local Area Connection 3 Properties
General
Authentication
Advanced
Select this option to provide authenticated network access for Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Protected EAP (PEAP)
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

5. Select the Enable IEEE 802.1x authentication for this network check box.
6. In the EAP type drop-down list, select Protected EAP (PEAP).
7. Select the Authenticate as computer when computer information is available check box.
8. Click Properties.

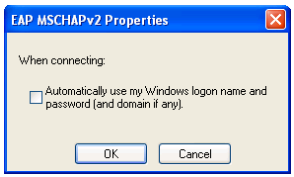
   The Protected EAP Properties dialog box appears.



9. Make sure that the Validate server certificate check box is selected.

10. In the Select Authentication Method drop-down list, select Secured password (EAP-MSCHAP v2).
11. If the user credentials for connecting to the Embedded NGX appliance differ from the user credentials for connecting to Windows, do the following:
    a. Click Configure.

       The EAP MSCHAPv2 Properties dialog box appears.



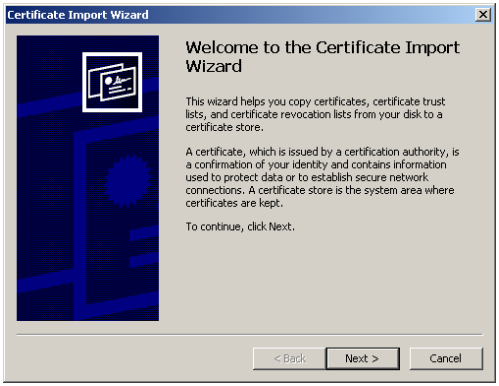
    b. Clear the check box.
    c. Click OK.
12. Click OK in all open windows.

Installing the Embedded NGX Appliance's CA Certificate on Clients

To install the Embedded NGX appliance's CA certificate on a client

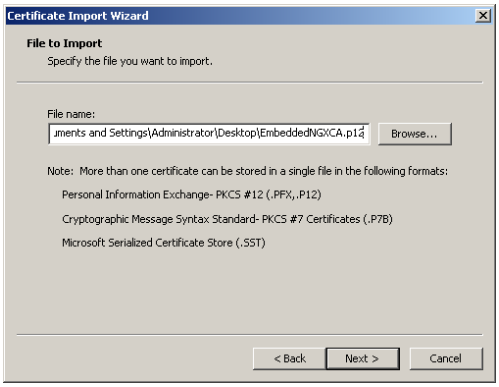
1. On the client, right-click on the Embedded NGX appliance's CA certificate, and click Install PFX in the pop-up menu that appears.

   The Certificate Import Wizard opens displaying the Welcome to Certificate Import Wizard screen.


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

2. Click Next.

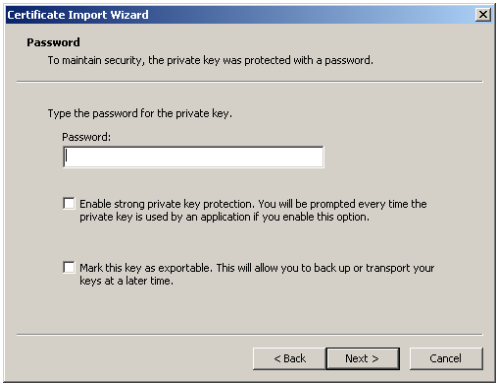
   The File to Import dialog box appears.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
uments and Settings\Administrator\Desktop\EmbeddedNGXCA.p12
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

3. Browse to the Embedded NGX appliance's CA certificate (*.p12 file).

4. Click **Next**.

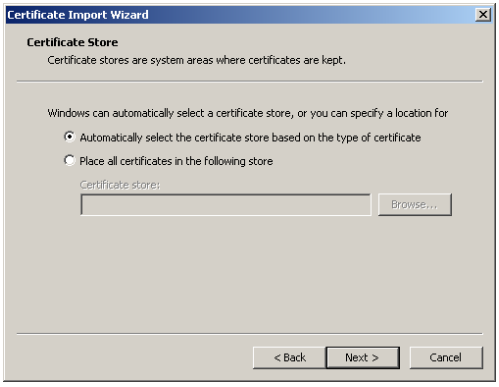
   The **Password** dialog box appears.


Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
< Back
Next >
Cancel

   Do not type a password.

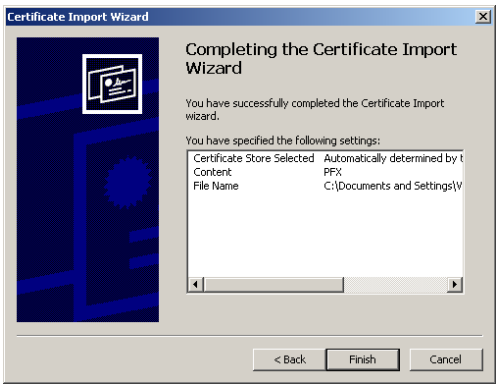
5. Click **Next**.

   The **Certificate Store** dialog box appears.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

6. Click **Automatically select the certificate store based on the type of certificate**.
7. Click **Next**.

The Completing the Certificate Import Wizard screen appears.



8. Click Finish.

   If the Embedded NGX appliance certificate was self-signed, a warning message appears.

Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
CA-00:08:da:77:70:70
Windows cannot validate that the certificate is actually from "CA-00:08:da:77:70:70". You should confirm its origin by contacting "CA-00:08:da:77:70:70". The following number will assist you in this process:
Thumbprint (sha1): 4240E3F0 A7EE46B7 D8CE5150 6763C48D 43D33F40
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

   Do the following:

   a. Click Yes.

      A success message appears.

   b. Click OK.

9. To check that the certificate was successfully installed as a trusted root CA, do the following:

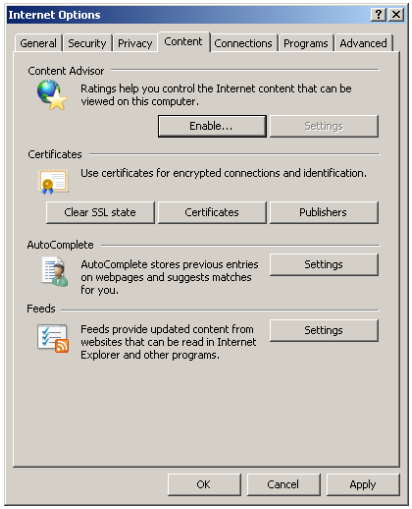
   a. On the client, open Internet Explorer.

   b. In the Tools menu, click Internet Options.

      The Internet Options dialog box appears displaying the General tab.

c. Click the **Content** tab.

The **Content** tab appears.

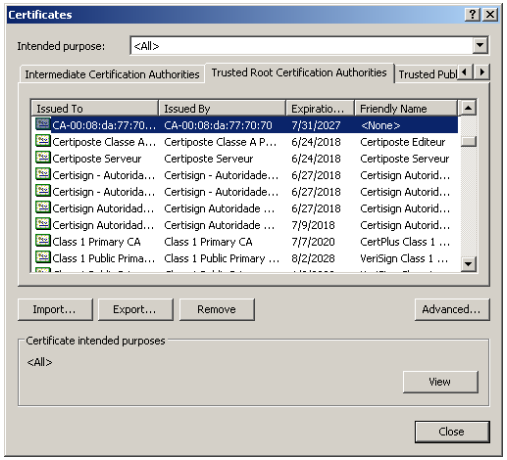


d. Click **Certificates.**

The **Certificates** dialog box appears.

e. Click the **Trusted Root Certification Authorities** tab.

The **Trusted Root Certification Authorities** tab appears.

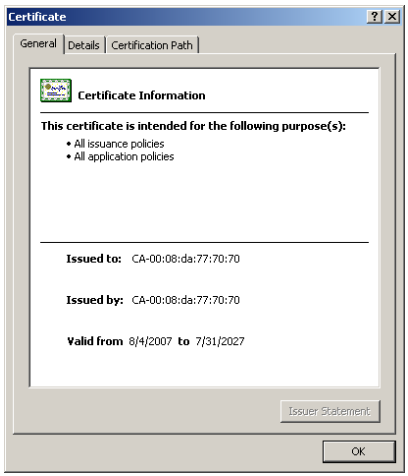


f. In the list, locate the Embedded NGX appliance's CA certificate.

The certificate's name is in the format `CA-<Identifier>`, where `<Identifier>` is the Embedded NGX appliance's MAC address or gateway name.

g. To view further information about the certificate, double-click on it.

The Certificate dialog box appears with additional information.



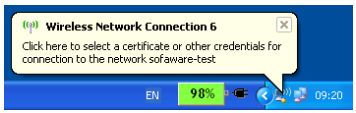
Connecting Wireless Clients to the Embedded NGX Appliance

To connect a wireless client to the Embedded NGX appliance

1. In the START menu, click Control Panel.
2. Click Network Connections.

   A list of wireless networks appears.
3. Select the Embedded NGX appliance wireless network.
4. Click Connect.

A popup message appears asking you to supply credentials.


Wireless Network Connection 6
Click here to select a certificate or other credentials for connection to the network sofaware-test
EN
98%
09:20

5. Click on the popup message.

   The Enter Credentials dialog box appears.

6. Type the Network Access user's user name and password in the fields provided.
7. Click OK.

   The wireless client attempts to connect to the network.

   Upon successful connection, the client indicates that it is connected to the network.